COLLEGE POLICY: 471

DATA PROTECTION STANDARDS

Purpose and Overview

As an employee of UA Cossatot, you have access to data and sensitive information about students and employees, including personally identifiable information (PII). PII is information that can be used on its own or in combination with other information to identify a specific individual. PII includes names, addresses, phone numbers, social security numbers, passport information, genetic profiles, academic information, healthcare information, employment records, etc.
Breach or loss of data in higher education can be very costly and largely depends on the type and amount of data breached. The cost of a data breach can reach millions of dollars and can result in the loss state/federal funding, including Title III/Title IV funds.

All UA Cossatot employees have a responsibility to ensure that all personal data is:

- Is obtained fairly and stored securely.
- Is kept confidential is not disclosed to unauthorized personnel or third parties.
- Is used and shared both appropriately and legally.
- If applicable, is disposed of properly when no longer required.

As an institution of higher education, we must comply to the guidelines set forth in the following privacy regulations and laws:

- **Family Education Rights and Privacy Act (FERPA)** - Designed to protect students and their families by ensuring the privacy of student educational records. If you have been assigned access to student information, you need to be aware of FERPA regulations and the consequences of violating FERPA regulations. The Family Educational Rights and Privacy Act of 1974 (as amended), sets forth requirements regarding the privacy of student records. This law applies to postsecondary institutions as well as K-12 schools.

- **Gramm-Leach Bliley Act (GLBA**) - Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data. Although we are not a financial institution, it was determined in 2017 by the federal Office of Management and Budget (OMB) and the Department of Education's Federal Student Aid (FSA) that colleges and universities must follow the GLBA safeguard guidelines. GLBA compliance will be included in any FSA audits.

- **General Data Protection Regulation (GDPR)** - is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.

The need to protect the privacy and integrity of our data requires that all access to the Student Information System (SIS)/Enterprise Resource Planning (ERP), at any level, be limited only to those users with a legitimate need-to-access. All user accounts will be created based on the principal of least privilege. Following this principle means that the least level of access, or permissions, necessary to do a job or task will be granted to a user.

Please consider the following rules to ensure data safety and security:

- Use strong, difficult to guess passwords. Use a combination of both upper/lower case letters, numbers, and special characters. Never use the same password for multiple accounts.
- Never share your username and password, under any circumstances, with anyone else. This is strictly prohibited and could result in immediate termination.
- Always lock or log out of your computer when leaving your work area. Staying logged in may allow unauthorized users access to sensitive information.
- Any device with access to SIS/ERP data should only be used by employees of the college with a legitimate need to access. Do not allow students, children, family members, community users, etc. access to these devices.
- Adopt and adhere to a clean desk policy. This means passwords are not written down and stored in locations where it is easily accessible to others. Make sure you keep all documents, files, identification cards, etc. that may contain any personally identifiable information (PII) about a student or employee securely locked away in your desk or file cabinet.
- Personal information should never be transported or stored in off campus locations. Do not save personal information to removable storage devices unless there is a legitimate need and the external storage device has encryption enabled. Do not leave college owned devices unattended in public locations or in vehicles.
- Devices accessing potentially sensitive or confidential information, must have disk drive encryption enabled.
- Remote access to SIS/ERP systems must be secured via virtual private network (VPN). Never use open/public wireless connections to access private information.
- Manipulation of data other than what is required to perform your job duties is strictly prohibited.

Failure to comply with the Data Protection Standards may result in harm to individuals, organizations, or UA Cossatot. The unauthorized or unacceptable use of data, including the failure to comply with these standards, constitutes a violation of UA Cossatot policy and may subject the user to revocation of the privilege to use UA Cossatot systems or disciplinary action, up to and including termination of employment.

Data Protection, Backup, and Recovery

Unless otherwise indicated, the following backup and recovery policies will apply.

a. SIS Server/POISE. The SIS server is backed up daily. One copy of the data is backed up remotely to the Jenzabar datacenter. Another copy of the data is backed up to tape and media is stored offsite in our safe deposit box at Farmers Bank and Trust. Backup tapes are rotated daily with a monthly archive tape also stored in the safe deposit box.

b. Docubase (Document Imaging/Workflow)– Docuabse is backed up daily with three immutable copies stored remotely using the Dell Apex backup solution.

c. Windows Servers (Physical and Virtual) – All Windows servers are backed up daily with three immutable copies stored remotely using the Dell Apex backup solution.

d. Office 365 Data– Office 365 user data (Exchange Online, SharePoint Online, Microsoft Teams, and OneDrive) is backed up daily with three immutable copies stored remotely using Dell Apex backup solution.

e. Network Shares – All file server data is backed up daily with three immutable copies stored remotely using the Dell Apex backup solution.

f. Local User Data – Data stored locally on user devices (laptops, desktops, etc.) is not backed up. Local data that needs to be backed up should be stored in OneDrive.

Responsibilities

IT staff is responsible for the following:

a. Determine and execute the appropriate data protection procedures to comply with this policy.

b. Determine and implement the appropriate protection procedures for hardware, software, and related technologies.

c. Monitor daily operations as it relates to data protection and backup procedures.

d. Perform periodic testing of data recovery capabilities.

e. Keep all systems and software updated and patched.

Policy History:
November 7, 2022

PROCEDURE: NONE